

REMARKS

Claims 1-57 are pending, with claims 1, 12, 19, 23, 34, 41, 45 and 56 being independent. Claims 1, 23 and 56 have been amended. No new matter has been added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Information Disclosure Statement

The present application was filed with an information disclosure statement on October 31, 2003. Consideration of this originally submitted information disclosure statement is requested, along with the Examiner's initials and signature on the 1449 form provided.

Rejections Under 35 U.S.C. §§ 102 & 103

Claims 1-8, 10-17, 19-30, 32-39 and 41-57 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by US Patent No. 7,178,033 to Garcia. Claims 9, 18, 31 and 40 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Garcia, and further in view of DeMarines (NPL "Authentica: Content Security for the Enterprise"). These contentions are respectfully traversed.

Prior to its amendment herein, claim 1 recited, "receiving a request from a client; and pre-authorizing the client, in response to the request, to allow actions by a user as a member of a group of users by sending to the client offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document." (Emphasis added.) The fact

that pre-authorization is performed to allow actions by a user as a member of a group of users is very important, and this aspect of the claimed subject matter is described throughout the Specification. *See e.g.*, the Specification at ¶s 50 and 120. This allows a user to be pre-authorized to access secured electronic documents based on that user's membership in a defined group of users. As described in one example in the Specification, "an ACE [Access Control Entry] can specify that 'only members of the public relations staff may view a document before its release date, after which anyone can view the document.'" *See* the Specification at ¶ 87. In other words, a key used for a whole group of users can be downloaded onto the computer of a user from that group and thereafter be used to give that user access (in view of the user's group membership) to a secured document that is accessed for the first time while offline. *See e.g.*, the Specification at ¶ 20.

The problem addressed by the present invention relates to how a system can efficiently pre-authorize a client to allow offline access to a secured document when that document is first opened by the user when the client is offline. As discussed in the Background:

Traditional document control systems have included servers that store and manage encryption keys for documents secured by the system, providing persistent protection for documents by requiring the server to be contacted before a secured document can be opened. Such systems have also provided offline capabilities by caching a cryptographic document key on a client to allow the client to open a document for a limited time when the user is offline, provided the document is first opened while online.

See Specification at ¶ 2 (emphasis added). The claimed subject matter addresses this problem by employing two keys, a first key associated with a group of users and a second key associated

with a document, and performing updates to the group keys (including the first key) at opportune times, in accordance with a client server protocol. When online, the system automatically caches a copy of the first key (the user group key), which can then be used later on (while offline) to decrypt the second key, which can be used to decrypt a document (e.g., a document that was received in an email, but not opened until the client was offline). *See e.g.*, the Specification at ¶s 117-121, and FIG. 11.

Garcia does mention the use of group keys, but Garcia does not specify the process by which those group keys are updated in the event of changes to user group membership, and Garcia is clearly focused on requiring connection to a network to pass an access test when a document is opened for the first time.

To access the contents in the encrypted data portion 112, one needs to obtain the file key to decrypt the encrypted data portion 112. To obtain the file key, one needs to be authenticated to get a user or group key and pass an access test in which at least the access rules in the security information are measured against the user's access privilege (i.e., access rights).

See Garcia at col. 8, lines 1-7 (emphasis added). This and other portions of the document security techniques of Garcia make clear that Garcia does not in any way teach or suggest pre-authorizing a client to access an electronic document for the first time when offline, as recited in claim 1. To further emphasize this distinction, claim 1 has been amended to clarify that, "the first key being useable at the client to access an electronic document while offline by decrypting a second key in the electronic document." (Emphasis added.) Thus, for all of the above reasons, independent claim 1 should be allowable over Garcia.

Independent claim 12 should be allowable over Garcia for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, “receiving from a document control server, when online, offline access information comprising a first key associated with a group of users of the document control server; and allowing access to an electronic document, when offline, by performing operations comprising using the first key to decrypt a second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document.” (Emphasis added.)

Independent claim 19 should be allowable over Garcia for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, “encrypting an electronic document; and incorporating into the encrypted electronic document an address of a document control server, document-permissions information, and an encryption key useable in decrypting the encrypted electronic document, the encryption key being encrypted with a key generated by, and associated with a group of users of, the document control server.” (Emphasis added.)

Independent claims 23, 34 and 41 should be allowable over Garcia based on the arguments presented above with respect to claims 1, 12 and 19.

Independent claim 45 should be allowable over Garcia for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, “a document control server that synchronizes offline access information with a client in response to a client request, the offline access information comprising a first key associated with a group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document; and the client that allows access to the electronic document, when offline, by a user as

a member of the group, using the first key to decrypt the second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document.” (Emphasis added.)

Independent claim 56 should be allowable for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, “server means for transparently providing offline access information for controlled documents to pre-authorize a client to allow actions by a user as a member of a group of users, the offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document while offline by decrypting a second key in the electronic document; and client means for accessing the electronic document using the offline access information.” (Emphasis added.)

DeMarines fails to cure the noted deficiencies of Garcia, even if DeMarines is combinable with Garcia (which is not conceded). Thus, for all of the above reason, each of independent claims 1, 12, 19, 23, 34, 41, 45 and 56 should be in condition for allowance. Dependent claims 2-11, 13-18, 20-22, 24-33, 35-40, 42-44, 46-55 and 57 should be allowable based on their dependence from allowable base claims and the additional recitations they contain. For example, claims 3 and 25 recite, “comparing current user-group information for the user with received user-group information for the user from the client.” The cited portion of Garcia fails to teach or suggest this subject matter, which can facilitate rapid synchronization of group keys between a server and a client. Thus, these claims should be allowable for at least this additional reason.

Claims 6 and 28 recite, "wherein receiving a request comprises receiving a request from the client to take an action with respect to a second document." As described in the Specification:

The request 1130 can be any type of request sent to the server 1120 periodically, such as a request from the client 1110 to take an action with respect to a document 1135, which may be located at the client 1110 or elsewhere and may be a secured document or not. The server 1120 can verify an authenticated user at the client 1110 in connection with the request 1130, and this verification of an authorized user can cause the synchronization operation to initiate. For example, the server 1120 can be a server such as any described above, and the synchronization operation can piggyback on other operations that use authentication (e.g., when a user attempts to access or secure a document while online). Alternatively, synchronization can occur without prior authentication; the server 1120 can encrypt the offline access information using the user's public key so that only the user can decrypt them; the encrypted offline access information can be retained by the client 1110, and when the user next attempts to open a document, the retained information can be decrypted and used to update the client's secure local database as described further below.

See Specification at ¶ 119, and FIG. 11 (emphasis added). In other words, the request that triggers the pre-authorization for access to an electronic document can be completely unrelated to that electronic document. This approach to key management represents a significant improvement over prior systems because the ability to access many documents offline can be quickly updated in a client machine by simply caching a set of user group keys, at opportune times, and these group keys can then be used to open any number of documents that have their document keys encrypted with a given group key cached on the client. Nothing in Garcia

teaches or suggests this approach to offline access as presently claimed. Thus, these claims should be allowable for at least this additional reason.

Claims 8 and 30 recite, "wherein the offline access information further comprises: at least one user-specific key; at least one group-specific key, including the first key; and at least one set of document-permissions information associated with multiple documents." Garcia fails to teach or suggest this subject matter, which can provide additional flexibility in how offline access to a document can be effected. Note that both the user key and the group key can be independently useable at the client to access a given document. See the Specification at ¶ 131. Thus, these claims should be allowable for at least this additional reason. Dependent claims 15, 37 and 48 also include similar features and should be allowable for similar reasons.

Claim 11 recites, "wherein the offline access information further comprises at least one set of document-permissions information associated with a specific document selected based on synchronization prioritization information." Garcia fails to teach or suggest this subject matter, which can facilitate synchronization by dividing synchronization operations based on priority (e.g., higher priority synchronizations are performed first). Thus, this claim should be allowable for at least this additional reason. Dependent claim 33 also includes similar subject matter and should be allowable for similar reasons.

Conclusion

The foregoing comments made with respect to the positions taken by the Examiner are not to be construed as acquiescence with other positions of the Examiner that have not been explicitly contested. Accordingly, the above arguments for patentability of a claim should not be

Applicant : Bill Shapiro, et al.
Serial No. : 10/699,124
Filed : October 31, 2003
Page : 23 of 23

Attorney's Docket No.: 07844-621001 / P572

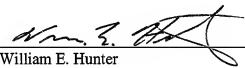
construed as implying that there are not other valid reasons for patentability of that claim or other claims.

A notice of allowance is respectfully requested. No fees are believed due with this response. However, please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: _____

Sept. 21, 2007



William E. Hunter
Reg. No. 47,671

Fish & Richardson P.C.
PTO Customer No. 021876
Telephone: (858) 678-5070
Facsimile: (858) 678-5099